

Asymmetric Latin squares, Steiner triple systems, and edge-parallelisms

Peter J. Cameron*

This article, showing that almost all objects in the title are asymmetric, is re-typed from a manuscript I wrote somewhere around 1980 (after the papers of Bang and Friedland on the permanent conjecture but before those of Egorychev and Falikman). I am not sure of the exact date. The manuscript had been lost, but surfaced among my papers recently.

I am grateful to Laci Babai and Ian Wanless who have encouraged me to make this document public, and to Ian for spotting a couple of typos. In the section on Latin squares, Ian objects to my use of the term “cell”; this might be more reasonably called a “triple” (since it specifies a row, column and symbol), but I have decided to keep the terminology I originally used.

The result for Latin squares is in

B. D. McKay and I. M. Wanless, On the number of Latin squares, *Annals of Combinatorics* **9** (2005), 335–344 (arXiv 0909.2101)

while the result for Steiner triple systems is in

L. Babai, Almost all Steiner triple systems are asymmetric, *Annals of Discrete Mathematics* **7** (1980), 37–39.

*My address when I wrote this paper was Merton College, Oxford OX1 4JD, UK. My current address is School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews, Fife KY16 9SS, UK.

1 Introduction

Recently, Bang [1] and Friedland [3] have shown that the permanent of a doubly stochastic matrix of order n is at least e^{-n} . This result substantially improves known lower bounds for the numbers of combinatorial structures of the types mentioned in the title. (It is already documented in the literature [6, 8, 2] that such improvement would follow from the truth of the van der Waerden permanent conjecture; the result of Bang and Friedland is close enough to the conjecture to have the same effect.) In this paper, I give a possibly less well-known consequence of the result on permanents.

Theorem 1 *Almost all Latin squares, Steiner triple systems, or edge-parallelisms of complete graphs have no non-trivial automorphisms; that is, the proportion of such objects of an admissible order n admitting non-trivial automorphisms tends to zero as $n \rightarrow \infty$.*

Here, as is well-known, n is admissible for Steiner triple systems if and only if $n \equiv 1$ or $3 \pmod{6}$, and n is admissible for edge-parallelisms if and only if $n \equiv 0 \pmod{2}$. All integers are admissible orders of Latin squares. The paper concludes with the observation that a similar result holds for strongly regular graphs with least eigenvalue -3 or greater.

I am grateful to J. H. van Lint for helpful discussions on permanents.

2 Latin squares

Given an $n \times (n - k)$ Latin rectangle, the number of ways of choosing an $(n - k + 1)^{\text{st}}$ row is the permanent of a $(0, 1)$ matrix of order n with row and column sums k (see Ryser [6]), and hence is at least $(k/e)^n$ (by [1, 3]). So the number of Latin squares of order n is at least $\prod_{k=1}^n (k/e)^n = (n!)6/e^{n^2}$. This number is greater than $n^{(1-\varepsilon)n^2}$ for $n \geq n_0(\varepsilon)$.

We take the most general definition of an automorphism of a Latin square S , as a permutation on the $3n$ symbols indexing the rows, columns and entries (say $\{r_1, \dots, r_n, c_1, \dots, c_n, e_1, \dots, e_n\}$) preserving the obvious partition into three sets R, C, E of size n and also the set of triples (r_i, c_j, e_k) for which the (i, j) entry of S is k . (We call such triples *cells*.) If an automorphism fixes elements in at least two of R, C, E , then its fixed elements form a subsquare of S . Note that the order of a subsquare is at most $\frac{1}{2}n$.

Now let g be one of the $6(n!)^3$ permutations of $R \cup C \cup E$ fixing the partition. How many Latin squares admit g as an automorphism? If g doesn't fix the three sets R, C, E , then it fixes at most n cells of any such square (for any fixed cell on r_i must also be on c_j , if $g(r_i) = c_j$, and r_i and c_j determine a unique cell; similar arguments in the other cases). If g is not the identity but fixes the three sets then, as remarked earlier, it fixes at most $\frac{1}{4}n^2$ cells. For $n \geq 4$, we have $n \leq \frac{1}{4}n^2$.

Let r be the number of fixed cells (determined by their rows and columns). We may choose their entries in at most n^r ways. Any choice of entry for a non-fixed cell determines all the cells in its orbit under g ; so there are at most $n^{\frac{1}{2}(n^2-r)}$ of these. So the number of fixed squares is at most $n^{\frac{1}{2}(n^2+r)} \leq n^{5n^2/8}$.

Hence the number of Latin squares admitting non-trivial automorphisms is at most $6(n!)^3 n^{5n^2/8} = o((n!)^n / e^{n^2})$.

3 Steiner triple systems

The number of Steiner triple systems of admissible order n is at least $n^{(1-\varepsilon)n^2/6}$ for sufficiently large n (combining Wilson's results [8] with those of Bang and Friedland).

Let g be a non-identity automorphism of a Steiner triple system S of order n , and suppose g fixes m points. The fixed points carry a subsystem of S , so $m \leq \frac{1}{2}(n-1)$. This subsystem contains $m(m-1)/6$ fixed blocks. Any other point lies in at most one fixed block, so at most $\frac{1}{2}(n-m)$ further blocks are fixed. The total number of fixed blocks is thus at most $(n^2 + 2n - 9)/24$, and the number r of block-orbits satisfies

$$\begin{aligned} r &\leq (n^2 + 2n - 9)/24 + \frac{1}{2}(n(n-1)/6 - (n^2 + 2n - 9)/24) \\ &< 5n^2/48. \end{aligned}$$

Now take a permutation g on the set of points. Choose triples for the blocks of a Steiner triple system admitting g in such a way that, when any new block is chosen, its entire orbit under g is included. The number of such sequences of blocks is at most $\binom{n}{3}^r < (n^3/6)^r$; so the number of Steiner triple systems is at most $(n^3 e / 6r)^r$.

Now $(a/x)^x$ is an increasing function of x for $x < ae$; so, since $r \leq 5n^2/48$, we have that $(n^3 e / 6r)^r \leq (8ne/5)^{5n^2/48}$. Hence the number of Steiner triple systems admitting non-trivial automorphisms is at most $n!(8ne/5)^{5n^2/48} = o(n^{(1-\varepsilon)n^2/6})$.

4 Edge-parallelisms

The structures considered here are sometimes referred to as 1-factorisations or minimal edge-colourings of complete graphs; they are partitions of the 2-subsets of an n -set X into “parallel classes”, each of which partitions X . For a general reference, see [2, Chapter 4]. It follows from [2] together with the result of Bang and Friedland that, if n is admissible (that is, even), the number of edge-parallelisms of order n is at least $n^{(1-\varepsilon)n^2/2}$ for $n \geq n_0(\varepsilon)$.

We need the fact that the number of 1-factors of a k -valent graph on n vertices is at most $k^{\frac{1}{2}n}$ (see [2, p. 64]).

Lemma 1 *Let Γ be a k -valent graph on n vertices, g an automorphism of Γ with no fixed vertices. Then the number of 1-factors of Γ fixed by g is at most $(8ek)^{\frac{1}{4}n}$.*

Proof Count fixed 1-factors containing r edges fixed by g . The fixed edges are 2-cycles of g , so there are at most $\binom{\frac{1}{2}n}{r}$ choices for these. Suppose the non-fixed edges lie in m orbits under g . Choosing these in order, such that each new edge chosen is followed by its orbit, we have at most $((\frac{1}{2}n - r)k)^m$ choices; hence at most $((\frac{1}{2}n - r)k)^m / m! < ((\frac{1}{2}n - r)ke/m)^m$ choices up to permutations of the orbits. As in the last section, this number is greatest when m has its largest possible value $\frac{1}{2}(\frac{1}{2}n - r)$, and so it is smaller than $(2ek)^{\frac{1}{2}(\frac{1}{2}n - r)}$. Now the total number of 1-factors is less than

$$\sum_{r=0}^{\frac{1}{2}n} \binom{\frac{1}{2}n}{r} (2ek)^{\frac{1}{2}(\frac{1}{2}n - r)} \leq 2^{\frac{1}{2}n} (2ek)^{\frac{1}{4}n} = (8ek)^{\frac{1}{4}n}.$$

Now we turn to the proof of the theorem. Suppose g is a permutation of an n -set; we want to count edge-parallelisms fixed by g . If g fixes r points, with $r > 0$, then its fixed points carry a subsystem, whence $r \leq \frac{1}{2}n$ ([2, p. 25]), and it fixes $r - 1$ parallel classes (1-factors). So the number of orbits of g on parallel classes satisfies $m \leq r + \frac{1}{2}(n - r) \leq \frac{3}{4}n$. There are at most $n^{\frac{1}{2}n}$ 1-factors altogether, and so at most $n^{3n^2/8}$ fixed edge-parallelisms.

Now suppose that g fixes no points; count fixed edge-parallelisms with s fixed parallel classes. By the lemma, the fixed parallel classes can be chosen in at most $(8en)^{\frac{1}{4}ns}$ ways. If the remaining classes fall into m orbits, then $m \leq \frac{1}{2}(n - s)$, and as before there are at most $n^{\frac{1}{4}n(n-s)}$ choices for these. Multiplying, and summing over

s , we obtain at most $n(8en)^{\frac{1}{4}n^2}$ fixed edge-parallelisms. This number is smaller than $n^{3n^2/8}$ for sufficiently large n .

Thus the number of edge-parallelisms admitting non-trivial automorphisms is at most $n!n^{3n^2/8} = o(n^{(1-\varepsilon)\frac{1}{2}n^2})$.

5 Strongly regular graphs

Ray-Chaudhuri [5] and Neumaier [4] have shown that all but finitely many strongly regular graphs with least eigenvalue -3 are of one of the following types:

- (i) complete multipartite with block size 3;
- (ii) a Latin square graph (whose vertices are the cells of a Latin square, two vertices adjacent if the cells agree in row, column or entry);
- (iii) a Steiner graph (whose vertices are the blocks of a Steiner triple system, two vertices adjacent if the blocks intersect in a point).

For all but finitely many graphs of the second and third type, every graph-automorphism is induced by an automorphism of the Latin square or Steiner triple system. Moreover, all but finitely many strongly regular graphs with least eigenvalue greater than -3 are complete multipartite with block size 2, or square lattice or triangular graphs (Seidel [7]).

It follows that, of strongly regular graphs with least eigenvalue -3 or greater on at most n vertices, the proportion admitting non-trivial automorphisms tends to zero as $n \rightarrow \infty$.

It would be interesting to know whether the same assertion holds without the restriction on the least eigenvalue.

References

- [1] T. Bang, On matrix functions giving a good approximation to the van der Waerden permanent conjecture, preprint no. 30, Copehnagen University, 1979.
- [2] P. J. Cameron, “Parallelisms of Complete Designs”, London Math. Soc. Lecture Notes **23**, Cambridge Univ. Pr., Cambridge, 1976.

- [3] S. Friedland, A lower bound for the permanent of a doubly stochastic matrix, *Ann. Math.* **110** (1979), 167–176.
- [4] A. Neumaier, Strongly regular graphs with least eigenvalue $-m$, to appear.
- [5] D. K. Ray-Chaudhuri, Uniqueness of association schemes, *Proc. Int. Colloq. Theorie Combinatorie*, 465–479, Accad. Naz. Lincei, Roma, 1977.
- [6] H. J. Ryser, Permanents and systems of distinct representatives, “Combinatorial Mathematics and its Applications”, 55–68, Univ. North Carolina Pr., Chapel Hill, 1969.
- [7] J. J. Seidel, Graphs and two-graphs, *Proc. Fifth Southeastern Conf. Combinatorics, Graph Theory, Computing*, 125–143, Congressus Numerantium X, Utilitas Math., Winnipeg, 1974.
- [8] R. M. Wilson, Nonisomorphic Steiner triple systems, *Math. Z.* **135** (1974), 303–313.